

REMARKS

Claims 1-28 are pending in this application. Claims 1-28 are rejected. Claims 1, 6, 12, 15, 20, and 26 are the independent claims. Claims 2, 8, 16 and 22 are amended.

Formal Drawings

Applicants note Examiner has not yet indicated whether the drawings submitted on August 1, 2003 are accepted or objected to. Applicants respectfully request an indication from the Examiner as to the status of the August 1, 2003 drawings.

Rejections under 35 U.S.C. §112

Claims 2, 3, 6, 9-10, 16, 17, 22, 23-24 are rejected under 35 U.S.C. §112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

The Examiner contends the use of the terms "response request ID" and "card company ID number" are unclear.

Section 2111 of MPEP states:

During patent examination, the pending claims must be "given their broadest reasonable interpretation consistent with the specification." >The Federal Circuit's *en banc* decision in *Phillips v. AWH Corp.*, 415 F.3d 1303, 75 USPQ2d 1321 (Fed. Cir. 2005) expressly recognized that the USPTO employs the "broadest reasonable interpretation" standard:

The Patent and Trademark Office ("PTO") determines the scope of claims in patent applications not solely on the basis of the claim language, but upon giving claims their broadest reasonable construction "in light of the specification as it would be interpreted by one of ordinary skill in the art." *In re Am. Acad. of Sci. Tech. Ctr.*, 367 F.3d 1359, 1364[, 70 USPQ2d 1827] (Fed. Cir. 2004). Indeed, the rules of the PTO require that application claims must "conform to the invention as set forth in the remainder of the specification and the terms and phrases used in the claims must find clear support or antecedent basis in the description so that the meaning of the terms in the claims may be ascertainable by reference to the description." 37 CFR 1.75(d)(1).

With respect to the term "response request ID", the Examiner states that it is "unclear whether it is a response, a request, or an ID" (*April 4, 2008 Office action*: p. 3). Applicants

respectfully submit that in light of the specification and based on the plain meaning of the term, a “response request ID” is an ID or identification that symbolizes a “response request”. With regard to why one skilled in the art would be able to recognize the term, “response request ID”, as indicating identification, Applicants note that, commonly, the term ID is issued to refer to an identification. Additionally, the term ID is usually added to the end of the other term being described by the ID. Wikipedia.org defines ID as a known quantity mapping to an unknown quantity (www.wikipedia.org). For example, in programming, “ERRID”, which stands for “error ID”, is commonly used. Even to one who has never seen the term before, it is recognized as referring to an identification number that points to or describes a specific error. The same applies to the term “student ID” which describes an ID identifying a student. Similarly, a “response request ID” is ID identifying a response request.

With respect to the term “response request” in the term “response request ID”, the meaning is also understood by those skilled in that art. The term “request” is often described by the word preceding it. For example, a “confirmation request” requests confirmation from a user. A “(new) feature request” is a request for a new feature, for example, to be added to a program. Similarly, a “response request” is a request for a response, for example, from the receiving party. Therefore, one skilled in the art would recognize the term, “response request ID”, to refer to an identification number mapping to a specific request for a response from a receiving party, in which the type of response is defined by at least the ID. Additionally, Applicants submit claims 2, 8, 16 and 22 have been amended to further clarify the meaning of the term “response request ID”.

With respect to the term “card company ID number”, the Examiner states that the definition of the term ‘card company’ is unclear (*April 4, 2008 Office action*: p. 3-4). With respect to the term “ID number” in the term “card company ID number”, for the same reasons mentioned above, Applicants submit one of ordinary skill in the art would recognize that a “card company ID number” is an ID number identifying a card company. With respect to the term “card company” in the term “card company ID number”, Applicants respectfully submit that based at least on paragraph [0087] of Applicants’ original specification, the term “card company” refers to a “related organization” capable of freely using the public key. Further, a public key, and therefore, a private key, corresponds to a single card company ID number. Since each card company ID number corresponds with one card company, each card company corresponds with a public key and a private key set (Applicants Original Specification: page 33, lines 3-5).

Moreover, Applicants submit the specific type of company “card company” refers to is inconsequential. Whether “card company” is a playing card company, an IC card manufacturing company, or another type of card company, a secret key and a public key are created corresponding to the ID number.

Accordingly, Applicants submit, the terms “response request ID” and “card company ID number” do “find clear support or antecedent basis in the description so that the meaning of the terms in the claims may be ascertainable by reference to the description” (37 CFR 1.75(d)(1)) and thus, they meet the requirements for claim language set out in the MPEP and 37 CFR §1.75(d)(1).

Therefore, Applicants respectfully request that the rejections of claims 2, 3, 6, 9-10, 16, 17, 22 and 23-24 under 35 U.S.C. §112 be withdrawn.

Rejections Under 35 U.S.C. § 103 – Azuma and Schneier

Claims 1-2, 4-8, 11-14 rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. Patent No. 6,704,608 (Azuma) in view of “Applied Cryptography, 2nd Edition” 1996, pg. 37 (Schneier).

To establish a *prima facie* case of obviousness, three basic criteria must be met. First, there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or to combine reference teachings. Second, there must be a reasonable expectation of success. Finally, the prior art reference (or references when combined) must teach or suggest all the claim limitations. The teaching or suggestion to make the claimed combination and the reasonable expectation of success must both be found in the prior art, and not based on applicant's disclosure. *In re Vaeck*, 947 F.2d 488, 20 USPQ2d 1438 (Fed. Cir. 1991).

Applicants respectfully submit that neither Azuma nor Schneier, alone or in combination, teach each of the limitations in claim 1. The Examiner asserts that the combination of the encryption method of Azuma with the signing method of Schneier teaches each of the limitations of claim 1. However, neither Schneier nor Azuma teach that **both** encryption and decryption are performed using **the same secret key** as claim 1 requires. Claim 1 recites:

“a decoding section configured to decode the input random number **based on the secret key**; an encryption section configured to encrypt the decoded random number **based on the secret key**” (Emphasis added).

The Examiner proposes combining Azuma and Schneier by replacing the encryption method of Azuma with the signing method of Schneier. Azuma teaches **decrypting** a numeral using a **secret key** and **encrypting** the numeral using a **public key** (Azuma: col. 20, ln. 1-3). Schneier teaches **encrypting** a document using a **private key** and decrypting a document using a **public key** (Schneier: pg. 37, *Signing Documents with Public Key Cryptography*). Thus, both Schneier and Azuma teach encrypting and decrypting using **different keys**, not the same secret key as claim 1 requires. Thus, even if Azuma is modified by the teachings of Schneier to encrypt with a secret key and decrypt with a secret key, neither Schneier nor Azuma teach **both encrypting and decrypting using the same secret key** as claim 1 requires. Accordingly, neither Azuma nor Schneier, alone or in combination, teach each of the limitations of claim 1 as is required to support a *prima facie* case of obviousness.

Further, Applicants respectfully submit that even though Schneier teaches encryption with a private key, there would be no motivation to modify Azuma to encrypt with the private key. As noted in Azuma, the purpose of the system of Azuma is to provide higher confidentiality, and therefore, the system has a larger load due to mutual authentication or data encryption to provide higher security (Azuma: col. 4, ln. 30-35). However, modifying Azuma to encrypt with the private key lowers the security of the system. Specifically, a number encrypted with the private key can be decoded with the corresponding public key, which can be known by all devices. Hence, the number encrypted with the private key is not secure. In comparison, the original process described by Azuma encrypts a number such that only the intended device is able to read it. In other words, Azuma encrypts with the public key such that only the private key is able to decode it. Hence, the number encrypted with the public key is secure. Therefore, the device described by the combination of Azuma and Schneier is less secure than the unmodified system of Azuma. Accordingly, one of ordinary skill in the art would not be motivated to combine Azuma and Schneier as the Examiner suggests.

For at least the reasons stated above, the Examiner cannot establish a *prima facie* case of obviousness with respect to claim 1 as is required to support a rejection under §103.

Additionally claims 6 and 12 contain limitations similar to those of claim 1. Accordingly, at least by virtue of their similarity to claim 1, the Examiner cannot establish a *prima facie* case of obviousness with respect to either of claims 6 and 12 as is required to support a rejection under §103.

Further claims 2, 4, and 5 depend from claim 1; claims 7, 8, and 11 depend from claim 6; and claims 13 and 14 depend from claim 12. Accordingly, at least by virtue of their dependence from claims 1, 6, and 12, the Examiner cannot establish a *prima facie* case of obviousness with respect to any of claims 2-5, 7, 8 11, 13 and 14 as is required to support a rejection under §103.

Therefore, Applicants respectfully request that this rejection of claims 1-2, 4-8, and 11-14 under 35 U.S.C. §103(a) be withdrawn.

Rejections Under 35 U.S.C. § 103 – Azuma, Schneier and Reece

Claims 3, 9 and 10 are rejected under 35 U.S.C. 103(a) as being unpatentable over Azuma in view of Schneier further in view of U.S. Patent Publication No. 2003/0150915 (Reece).

The deficiencies of Azuma and Schneier have been discussed above and are applicable here as well because claim 3 depends from claim 1; and claims 9 and 10 depend from claim 6. For at least the reasons stated above, the combination of Azuma and Schneier fails to teach each of the limitations in either of claims 1 and 6. Reece fails to remedy these deficiencies at least because Reece does not deal with encryption keys. Accordingly, at least in view of their dependency from claims 1 and 6, none of Azuma, Schneier and Reece, alone or in combination, teach or suggest each of the limitations in any of claims 3, 9 and 10. Consequently, the Examiner cannot establish a *prima facie* case of obviousness with respect to any of claims 3, 9 and 10 as is required to support a rejection under §103.

Therefore, Applicants respectfully request that this rejection of claims 3, 9 and 10 under 35 U.S.C. §103(a) be withdrawn.

Rejections Under 35 U.S.C. § 103 – Azuma, Schneier and Yu

Claims 15, 18-19, 20-21, 24, 25-27 are rejected under 35 U.S.C. 103(a) as being unpatentable over Azuma in view of Schneier further in view of U.S. Patent No. 6,067,621 (Yu).

The deficiencies of Azuma and Schneier have been discussed above and are applicable here as well because claim 15 contains limitations similar to those of claim 1, claim 20 contains limitations similar to those of claim 6, and claim 26 contains limitations similar those in both claims 1 and 6. For at least the reasons stated above, the combination of Azuma and Schneier fails to teach each of the limitations in either of claims 1 and 6. Yu fails to remedy these deficiencies at least because Yu does not disclose decrypting and encrypting a random number using the same

key. Accordingly, at least in view of their similarity to claims 1 and 6, none of Azuma, Schneier and Yu alone or in combination teach each of the limitations in any of claims 15, 20 and 26. Consequently, the Examiner has not established a *prima facie* case of obviousness with respect to any of claims 15, 20 and 26 as is required to support a rejection under §103.

Additionally, claims 18 and 19 depend from claim 15; claims 21, 24 and 25 depend from claim 20; and claim 27 depends from claim 26. Consequently, the Examiner has not established a *prima facie* case of obviousness, as is required to support a rejection under §103, with respect to any of claims 18, 19, 12, 24, 25 or 27, at least in view of their dependency from claims 15, 20 and 26.

Therefore, Applicants respectfully request that this rejection of claims 15, 18-19, 20-21, 24, and 25-27under 35 U.S.C. §103 be withdrawn.

Rejections Under 35 U.S.C. § 103 – Azuma, Schneier, Yu, and Reece

Claims 17, 23-24 are rejected under 35 U.S.C. 103(a) as being unpatentable over Azuma in view of Schneier further in view of Yu as applied to claim 15 above, and further in view of Reece.

The deficiencies of Azuma, Schneier, Reece and Yu have been discussed above and are applicable here as well because claim 17 depends from claim 15, and claims 23 and 24 depend from claim 20. For at least the reasons stated above, none of Azuma, Schneier and Yu, alone or in combination, teach each of the limitations in either of claims 15 and 20. Reece fails to remedy these deficiencies because Reece does not deal with encryption keys. Accordingly, at least in view of their dependency from claims 15 and 20, none of Azuma, Schneier, Reece or Yu, alone or in combination, teach each of the limitations in any of claims 17, 23 and 24. Consequently, the Examiner has not established a *prima facie* case of obviousness with respect to any of claims 17, 23 and 24 as is required to support a rejection under §103.

Therefore, Applicants respectfully request that this rejection of claims 17 and 23-24 under 35 U.S.C. §103 be withdrawn.

CONCLUSION

In view of the above, Applicant earnestly solicits reconsideration and allowance of all of the pending claims.

Should there be any matters that need to be resolved in the present application, the Examiner is respectfully requested to contact the telephone number of the undersigned below.

If necessary, the Commissioner is hereby authorized in this, concurrent, and future replies, to charge payment or credit any overpayment to Deposit Account No. 08-0750 for any additional fees required under 37 C.F.R. § 1.16 or under 37 C.F.R. § 1.17; particularly, extension of time fees.

Respectfully submitted,

HARNESS, DICKEY, & PIERCE, P.L.C.

By: 
Donald J. Daley, Reg. No. 34,313

P.O. Box 8910
Reston, Virginia 20195
(703) 668-8000

DJD/JHA: tlt